ITU Centres of Excellence Network for Europe

NRD Cyber Security

Face-to-face Training Course on

INCIDENT RESPONSE PRACTICE

Vilnius, Lithuania
17-20 September 2019

COURSE OUTLINE

COURSE DESCRIPTION

Title	Incident response practice, hands-on scenario-based training
Objectives	Deliver fundamental theoretical and practical skills to handle and respond to the computer security incidents using real life incident logs and investigation tools.
Dates	17-20 September 2019
Duration	4 days
Registration deadline	30 August 2019 (*if a visa is not requested)*
Training fees	USD 800
Requirement	Participants are required to bring a laptop with them
Course code	19WS24302EUR-E

LEARNING OUTCOMES

Upon completion of this training, participants will be able to:

- apply incident response general workflow principles;
- follow the incident response procedure by using RTIR tool;
- conduct basic analysis of email messages and retrieve actionable data from email headers;
- investigate incidents by executing the system event log analysis;
- carry on incident root cause analysis;
- perform basic network forensic analysis.

TARGET POPULATION

The course is designed for CIRT, SOC members, incident handlers, IT professionals and anyone who is interested in incident handling and response.

TUTORS/INSTRUCTORS

NAME OF TUTOR(S)/INSTRUCTOR(S)	CONTACT DETAILS
Marius URKIS NRD CIRT lead, cyber security incident handling and forensics expert	mu@nrdcs.lt
Rimtautas ČERNIAUSKAS Technical cyber security consultant and investigator	rc@nrdcs.lt
Lecturers have been working in numerous countries on strengthening national cybersecurity environments in Asia, Africa, Europe and South America.	

EVALUATION

Besides the final test score (60% of total), the participants will be evaluated according to their active participation in roundtables, exercises sessions and other course activities (30% of total), reflecting quantity of time spent on the training (10%).

TRAINING SCHEDULE AND CONTENTS / AGENDA

Agenda

Day of arrival	Time	Activity
16/09/2019 Monday	19.00	Welcome Reception
1st day	Time	Topics/Activities
17/09/2019 Tuesday	9:00 – 10:30	Session 1 • Introductions and expectations • Global view on incident handling
	10:30 – 11:00	Coffee break
	11:00 – 12:30	Session 2 • Incident management key components

		• Available information sources, such as zone-h, *shodan, pastebin*, host and network logs
	12:30 – 13:30	Lunch break
	13:30 – 15:00	<u>Session 3</u> • Incident triage: initial evaluation of the incident information, classification • Hands-on exercise relevant to session topic • Review of exercise results
	15:00 – 15:30	Coffee break
	15:30 – 17:00	<u>Session 4</u> • Hands-on exercise relevant to the topic of the day • Review of exercise results
2nd day	Time	Topics/Activities

18/09/2019 Wednesday	9:00 – 10:30	<u>Session 5</u>
		• Incident types, related to email usage overview:
		  • Spam;
		  • Phishing;
		  • malware delivery.

	10:30 – 11:00	Coffee break
	11:00 – 12:30	<u>Session 6</u> • Hands-on exercise related to phishing e-mails • Review of exercise results
	12:30 – 13:30	Lunch break
	13:30 – 15:00	<u>Session 7</u> • Malware delivery by e-mails: methods, detection and protection
	15:00 – 15:30	Coffee break
	15:30 – 17:00	<u>Session 8</u> • Hands-on exercise related to detection and analysis of the malicious e-mails • Review of exercise results
3rd day	Time	Topics/Activities
19/09/2019 Thursday	9:00 – 10:30	<u>Session 9</u> • Overview of log analysis tools
	10:30 – 11:00	Coffee break
	11:00 – 12:30	<u>Session 10</u> • Website vulnerabilities, attack methods and their reflections in the logs
	12:30 – 13:30	Lunch break
	13:30 – 15:00	<u>Session 11</u> • Hands-on exercise related to the topic of the day • Review of Exercise results
	15:00 – 15:30	Coffee break
	15:30 – 17:00	<u>Session 12</u>

		• Hands-on exercise to day topic • Review of Exercise results
4th day	Time	Topics/Activities
20/09/2019 Friday	9:00 – 10:30	Session 13 • Network traffic data collection and logging (network capture, netflows) • Malicious activity patterns in network traffic and their detection
	10:30 – 11:00	Coffee break
	11:00 – 12:30	• Hands-on exercise relevant to the day topic: collection of information, analysis, incident handling according to the procedures • Review of exercise results
	12:30 – 13:30	Lunch break
	13:30 – 15:00	• Final Test
	15:00 – 15:30	Coffee break
	15:30 – 17:00	• Sum up of training course • Q&A and feedback on training course

METHODOLOGY

The training course material is based on illustrative real-life cases and their analysis. The course will be delivered using lectures, case studies, roundtable and hands-on exercises.

Slide sets will be provided as well as access to online material will be granted where applicable.

COURSE COORDINATION

Course coordinator:	**ITU coordinator:**
Name: Ruta Jasinskiene Email address: ITUCoE@nrdcs.lt	Name: Ms Rosheen Awotar-Mauree Email address: Rosheen.awotar@itu.int

REGISTRATION AND PAYMENT

ITU Academy portal account

Registration and payment should be made online at the ITU Academy portal.
To be able to register for the course you **MUST** first create an account in the ITU Academy portal at the following address:
https://academy.itu.int/index.php/user/register.

Training registration

When you have an existing account or created a new account, you can register for the course online at the following link: https://academy.itu.int/index.php/training-courses/full-catalogue/incident-response-practice-hands-scenario-based-training

You can also register by finding your desired course in our training catalogue https://academy.itu.int/index.php/training-courses/full-catalogue.

Payment

1. **On-line payment**

A training fee of USD 800 per participant is applied for this training. Payments should be made via the online system using the link mentioned above for training registration at https://academy.itu.int/index.php/training-courses/full-catalogue/incident-response-practice-hands-scenario-based-training

2. **Payment by bank transfer**

   Where it is not possible to make payment via the online system, select the option for offline payment to generate an invoice using the same link as above. Download the invoice to make a bank transfer to the ITU bank account shown below. Then send the proof of payment/copy of bank transfer slip and the invoice copy to Hcbmail@itu.int and copy the course coordinator. **All bank transaction fees must be borne by the payer**.

   Failure to submit the above documents may result in the applicant not being registered for the training.

3. **Group payment**

Should you wish to pay for more than one participant using bank transfer and need one invoice for all of them, create an account as **Institutional Contact. Institutional Contacts** are users that represent an organization. Any student can request to be an institutional contact or to belong to any existing organization.

To do this, head to your profile page by clicking on the **"My account"** button in the user menu. At the bottom of this page you should see two buttons:

a. If you want to **become an institutional contact**, click on the "**Apply to be an Institutional Contact"** button. This will redirect you to a small form that will ask for the organization name. After you fill the name of the organization you want to represent, click on **"continue"** and a request will be created. An ITU Academy manager will manually review this request and accept or deny it accordingly.

b. If you want to **belong to an existing organization**, click on the **"Request to belong to an Institutional Contact"** button. This will redirect you to a small form that will ask you to select the organization you want to join from an organization list. After you select the correct organization, click on **"continue"**, a request will then be created. The Institutional Contact that represents that organization will manually accept or deny your request to join the organization.

ITU BANK ACCOUNT DETAILS:	
Name and Address of Bank:	UBS Switzerland AG Case postale 2600 CH 1211 Geneva 2 Switzerland
Beneficiary:	Union Internationale des Télécommunications
Account number:	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Amount:	USD 800
Payment Reference:	CoE-19WS24302EUR-E -WBS No. P.40595.1.08

4. Other method of payment

If due to national regulations, there are restrictions that do not allow for payment to be made using options 1 & 2 above, please contact the ITU coordinator for further assistance.

CERTIFICATES

Each fully registered participant who will successfully complete the course, based on the evaluation, will receive an ITU Certificate after the course.